

10:11:10
F7: Frank Hendrie

Page 8

Annual 47 C.F.R. S: 64.2009(e) CPNI Certification
EB Docket 06-36

Annual 64.2009(e) CPNI Certification: Liberty Contracting & Consulting, LLC
Date filed: 2/27/2009
Name of company covered Certification: Liberty Contracting & Consulting, LLC
Form 499 Filer ID: 826971
Name of signatory: Frank Hendrie
Title of signatory: President

I, Frank Hendrie [name of officer signing certification], certify that I am an officer of Liberty Contracting & Consulting, LLC (the company named above, herein referred to as "the company"), and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47 C.F.R. S: 64.2001 et seq., which is a subpart to implement section 222 of the Communications Act of 1934 as amended, 47 U.S.C. 222.

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements set forth in section 64.2001 et seq. of the Commission's rules. See attached accompanying statement for details.

The company has not been the subject of any action taken against it in the form of proceedings or petitions related to violation of CPNI, filed with state commissions, the court system, or at the Commission in the past year.

The company understands that it must report on any information that it has with respect to the processes pretexters are using to attempt to access CPNI, and what steps the company is taking to protect CPNI.

Note, the company recognizes "pretexting" as "the process in which personal information is obtained by fraudulent means including identity theft, selling personal data for profit, or using some other method for snooping for information whose release was not authorized by the owner of the information. See attached accompanying statement for details on how the applicant guards CPNI data against pretexting.

Signed X Frank Hendrie [signature]

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI and the company has received 0 number of customer complaints related to unauthorized access of CPNI, or unauthorized disclosure of CPNI, broken down by category or complaint as follows:


- (1). Instances of improper access by employees: 0 complaints
- (2). Instances of improper disclosure to individuals not authorized to receive the information: 0 Complaints
- (3). Instances of improper access to online information by individuals not authorized to view the information). 0 Complaints

If it was affirmative, above, the company would have provided summary of all customer complaints received in the past year concerning the unauthorized release of CPNI.

The company is aware of "Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services, CC Docket No. 96-115; WC Docket No. 04-36, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927 (2007)("EPIC CPNI Order"). See 47 U.S.C. S: 222".

The company understands "47 C.F.R. S: 64.2009(e) in that it states:

- (1). "A telecommunications carrier must have an officer, as an agent of the carrier, sign and file with the Commission a compliance certificate on an annual basis.
- (2). That the officer must state in the certification that he or she has personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the rules in this subpart.
- (3). That the carrier must provide a statement accompanying the certification explaining how its operating procedures ensure that it is or is not in compliance with the rules in this subpart.
- (4). That the carrier must include an explanation of any actions taken against data brokers and a summary of all customer complaints received in the past year concerning the unauthorized release of CPNI.
- (5). That this filing must be made annually with the Enforcement Bureau on or before March 1 in EB Docket No. 06-36, for data pertaining to the previous calendar year."

Signed X  [signature]

Attached Accompanying Statement

The following are the measures put in place by the carrier (herein referred to as "the company") to protect CPNI from pretexting. The company understands that the three common types of "pretexting" are **identity theft, selling personal data for profit without authorization by the owner or using some other method for snooping for information whose release was not authorized by the owner of the information.**

- I. Pretexting via identify theft
 - (A). Identify theft via theft of physical hardware containing CPNI Data
Guarding Measures:
The company utilizes physical security such as locks and security surveillance to protect physical hardware and limits physical access to authorized personnel. Also, certain portable hardware such as laptops have security features that provide additional security.
 - (B). Identify theft via hacking/virtual intrusion of systems that carry CPNI
Guarding Measures:
The company utilizes security software to detect and prevent unauthorized access via hacking and other virtual methods.
- II. Pretexting via some other method for snooping for information whose release was not authorized by the owner
 - (A). Snooping via social engineering/ impersonation/false identification
Guarding Measures:
The company's customer service personnel (*the individuals most likely to be the targets of social engineering*) have specific policies that they must follow to identify that they are in contact with the owner of the CPNI data prior to discussing or revealing CPNI.
 - (B). Snooping by personnel not authorized to access data
Guarding Measures:
The company limits access of CPNI to authorized personnel only.
- III. Pretexting by selling CPNI for profit without authorization by the owner
 - (A). Selling CPNI data by the company with other companies
Guarding Measures:
The company does not share CPNI data with other companies for marketing and profit purposes.
 - (B). Sharing CPNI data for profit/marketing purposes by the company with sister companies, subsidiaries, parent companies or joint venture entities
Guarding Measures:
See page 4 to 8 for details (items 1 to 18).

Attached Accompanying Statement

The following items (1) to (18) are how the company guards CPNI against pretexting in the form of selling CPNI for profit or marketing purposes by the company to its sister companies, subsidiaries, parent companies or joint venture entities but without authorization by the owner. In the event that the company was to sell or share CPNI with its affiliated entities for marketing or profit purposes, it would strictly abide by the following policies in compliance with FCC rules as outlined in section 222 of the Communications Act of 1934 as amended, 47 U.S.C. 222 (47 C.F.R. S: 64.2001 to 64.2011 et seq.).

How The Company Complies with 47 C.F.R. S: 64.2001-64.2011 et seq.

- (1). The company does not enable use, disclosure or permit access to CPNI for any marketing purposes to any persons, entities parties outside of the company without the specific consent of the customer that owns the CPNI data.
- (2). If the company wishes to share CPNI with any subsidiaries or parent companies of the company and the customer only subscribes to only 1 category of service offered by the company, the company will secure the consent of the customer prior to sharing that CPNI data with subsidiaries or parent companies of the company.
- (3). In most cases, the company will go a step above and try to secure the consent of the customer to share CPNI data with subsidiaries and parent companies of the company, regardless of whether customer subscribes to 1 or more than 1 type of service offered by the company.
- (4). The company will not utilize, disclose or permit access to CPNI data to identify or track customers that call competing service providers.
- (5). If the company requires customer consent for utilizing, disclosing or permitting access to CPNI data, the company will obtain consent through written, oral or electronic methods.
- (6). The company understands that carriers that rely on oral approval shall bear the burden of proving that such approval has been given in compliance with the Commission's rules.
- (7). The company has a policy in which any customer approvals obtained for the use, disclosing or utilization of CPNI data will remain in effect until the customer revokes or limits such approval or disapproval.